CLAIMS

What is claimed is:

1 A method for protecting software from unauthorized use on a computer system as using an external security device, the method comprising the steps of:

(a) encrypting the software to be protected using an encryption key, creating encrypted software;

(b) authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software; and

(c) sending the encryption key from the security device to the computer system for decryption of the software.

2 The method of claim 1 wherein step (a) further includes the steps of:

(i) using at least first and second pieces of information to generate an encryption key;

(ii) associating the first piece of information with the encrypted software; and

(iii) storing the second piece of information in the security device.

3 The method of claim 2 wherein step (b) further includes the steps of:

(i) sending the first piece of information associated with the encrypted software to the security device, and

(ii) using the first piece of information and the second piece of information to generate the encryption key in the security device.

4 The method of claim 1 further including the steps of:

generating a second encryption key using the first and second pieces of information;

providing the second encryption key with the encrypted software;

during software authorization, generating a second encryption key on the security device using the first and second pieces of information;

using the second encryption key to encrypt the first encryption key generated on security device prior to transmitting the first encryption key to the computer system; and

when the encrypted first encryption key is received on the computer system, using the second encryption key provided with the encrypted software to decrypt the first encryption key.

5 The method of claim 1 further including the steps of:

generating a random number on the computer system;

transmitting the random number to the security device along with the first piece of information;

scrambling the security key generated by the security device by performing a reversible mathematical operation on the encryption key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled encryption key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the encryption key after the encrypted scrambled encryption key is decrypted on the computer system.

6 The method of claim 1 further including the step of: using an initialization vector and a key as the first and second pieces of information.

7 The method of claim 6 further including step of: using a security key as the encryption key and a communications key as the second encryption key.

8 The method of claim 7 further including the step of: embedding a mathematical algorithm within the security device to create the communications key and the security key from the dynamic key and the initialization vector.

9 The method of claim 8 further including the step of: including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processors.

10 The method of claim 9 further including the step of: sharing memory between the security processor and the co-processors and decrypting the encrypted software in the shared memory.

11 The method of claim 10 further including the step of: preventing the software from running in any of the co-processors unless the software has first been decrypted by the security processor.

12 The method of claim 6 wherein the initialization vector is created from a checksum of encrypted software to be protected.

13 The method of claim 6 further including the step of: associating a product ID with the software and transferring the product ID to the security device along with the initialization vector.

14 The method of claim 13 further includes the step of: providing multiple storage locations within the security device to enable storing multiple dynamic keys and corresponding product IDs.

15 The method of claim 14 further includes the step of: using the product ID code to locate and select the appropriate dynamic key within the security device when receiving an authorization request.

16 A method for protecting software from unauthorized use on a computer system, the method comprising the steps of:

(a) using at least first and second pieces of information to generate an encryption key;

(b) encrypting the software using the encryption key;

(c) associating the first piece of information with the encrypted software;

(d) storing the second piece of information in a security device; and

(e) authorizing use of the software after the encrypted software is loaded on the computer system and the security device is coupled to the computer system by,

(i) sending the first piece of information associated with the encrypted software to the security device,

(ii) using the first piece of information and the second piece of information to generate the encryption key in the security device,

(iii) transmitting the encryption key from the security device to the computer system, and

(iv) decrypting the encrypted software with the encryption key for use on the computer system.

17 The method of claim 1 further including the step of:

(v) discarding the encryption key after decryption of the encrypted software.

18 The method of claim 17 further including the steps of:

generating a second encryption key using the first and second pieces of information;

providing the second encryption key with the encrypted software;

during software authorization, generating the second encryption key on the security device using the first and second pieces of information;

a using the second encryption key to encrypt the first encryption key generated on security device prior to transmitting the first encryption key to the computer system; and

when the encrypted first encryption key is received on the computer system, using the second encryption key provided with the encrypted software to decrypt the first encryption key.

19 The method of claim 1 further including the steps of:

generating a random number on the computer system;

transmitting the random number to the security device along with the first piece of information;

scrambling the encryption key generated by the security device by performing a reversible mathematical operation on the encryption key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled encryption key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the encryption key after the encrypted scrambled encryption key is decrypted on the computer system.

20 The method of claim 16 further including the step of: using an initialization vector and a key as the first and second pieces of information.

21 The method of claim 20 further including steps of: using a security key as the encryption key and a communications key as the second encryption key.

22 A method for protecting software from unauthorized use on a computer system, the method comprising the steps of:

(a) creating an initialization vector and a dynamic key;

(b) using the initialization vector and the dynamic key to generate a security key;

(c) using the security key and the initialization vector to generate a communication key;

(d) encrypting software using the security key to create encrypted software;

(e) creating a software package comprising the initialization vector, the encrypted software, the communications key, and an authentication program;

(f) storing the dynamic key in a security device;

(g) authorizing use of the software after the software package has been loaded on the computer system and the security device coupled to the computer system by

(i) sending the initialization vector to the security device,

(ii) in the security device, using the initialization vector and the store dynamic key to generate the security key and communication key,

(iii) encrypting the security key using the communication key,

(iv) sending the encrypted security key to the computer system as a response,

(v) using the communications key in the software package to decrypt encrypted security key, and

(vi) using the security key to decrypt the encrypted software for use on the computer system.

23 The method of claim 22 further including the steps of:

generating a random number on the computer system;

transmitting the random number to the security device;

scrambling the security key generated by the security device by performing a reversible mathematical operation on the security key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled security key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the security key after the encrypted scrambled security key is decrypted on the computer system.

24 A computer-readable medium containing program instructions for protecting software from unauthorized use on a computer system as an external security device, the program instructions for:

(a) encrypting the software to be protected using an encryption key, creating encrypted software;

(b) authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software; and

(c) sending the encryption key from the security device to the computer system for decryption of the software.

25 The computer-readable medium of claim 24 wherein instruction (a) further includes the instructions for:

(i) using at least first and second pieces of information to generate an encryption key;

(ii) associating the first piece of information with the encrypted software; and

(iii) storing the second piece of information in the security device.

26 The computer-readable medium of claim 25 wherein instruction (b) further includes the instructions for:

(i) sending the first piece of information associated with the encrypted software to the security device, and

(ii) using the first piece of information and the second piece of information to generate the encryption key in the security device.

27 The computer-readable medium of claim 26 further including the instructions for:

generating a second encryption key using the first and second pieces of information;

providing the second encryption key with the encrypted software;

during software authorization, generating a second encryption key on the security device using the first and second pieces of information;

a using the second encryption key to encrypt the first encryption key generated on security device prior to transmitting the first encryption key to the computer system; and

when the encrypted first encryption key is received on the computer system, using the second encryption key provided with the encrypted software to decrypt the first encryption key.

28 The computer-readable medium of claim 24 further including the instructions for:

generating a random number on the computer system;

transmitting the random number to the security device along with the first piece of information;

scrambling the security key generated by the security device by performing a reversible mathematical operation on the encryption key using the random number;

encrypting the scrambled encryption key and transmitting the encrypted scrambled encryption key to the computer system; and

performing a reverse of the reversible mathematical operation performed within the security device using the random number to descramble the encryption key after the encrypted scrambled encryption key is decrypted on the computer system.

29 The computer-readable medium of claim 25 further including the instruction for: using an initialization vector and a key as the first and second pieces of information.

30 The computer-readable medium of claim 29 further including instruction for: using a security key as the encryption key and a communications key as the second encryption key.

31 The computer-readable medium of claim 30 further including the instruction for: embedding a mathematical algorithm within the security device to create the communications key and the security key from the dynamic key and the initialization vector.

32 The computer-readable medium of claim 31 further including the instruction for: including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processors.

33 The computer-readable medium of claim 32 further including the instruction for: sharing memory between the security processor and the co-processors and decrypting the encrypted software in the shared memory.

34 The computer-readable medium of claim 33 further including the instruction for: preventing the software from running in any of the co-processors unless the software has first been decrypted by the security processor.

35 The computer-readable medium of claim 25 wherein the initialization vector is created from a checksum of encrypted software to be protected.

36 The computer-readable medium of claim 29 further including the instruction for: associating a product ID with the software and transferring the product ID to the security device along with the initialization vector.

37 The computer-readable medium of claim 36 further includes the instruction for: providing multiple storage locations within the security device to enable storing multiple dynamic keys and corresponding product IDs.

38 The computer-readable medium of claim 37 further includes the instruction for: using the product ID code to locate and select the appropriate dynamic key within the security device when receiving an authorization request.

39 A computer software authentication system comprising:

a computer system;

a software package loaded on the computer system that includes,

an encrypted software program encrypted with a first encryption key,

an authorization program,

a first key of a keyset, and

a second encryption key; and

a security device in communication with the computer system that includes a second key of the keyset and mathematical algorithms,

wherein when the software package is executed the computer system, the encrypted software program is authenticated by,

transferring the first key of the keyset from the authorization program to the security device,

generating in the security device the first and second encryption keys using the keyset and the mathematical algorithms,

encrypting the first encryption key using the second encryption key,

transferring the encrypted first encryption key from the security device to the computer system,

decrypting the encrypted first encryption key on the computer system using the second encryption key included in the software package, and

using the first encryption key to decrypt the encrypted software for execution on the computer system.